ECS Configuration Change Request

1. Originator	2. Log Date:	3. CCR #:	4. Rev:	5. Tel:	6. Rm #:	7. Dept.
Henry Baez	05 OCT 00	00-0980	—	925-1025	2101D	SED

8. CCR Title: Install test executable to fix telnetd daemon security bug on IRIX 6.2 and 6.5.x machines.

9. Originator Signature/Date	10. Class	11. Type:	12. Need Date:
Henry Baez 10/4/2000	II	CCR	10-10-2000

13. Office Manager Signature/Date	14. Category of Change:	15. Priority: (If "Emergency" fill in Block 28).
Randy Hayes 10/4/2000	Initial ECS Baseline Doc.	Emergency

16. Documentation/Drawings Impacted:	17. Schedule Impact:	18. CI(s) Affected:
911-TDA-004, 911-TDA-005, 920-TDx-014		

19. Release Affected by this Change:	20. Date due to Customer:	21. Estimated Cost:
5A, 5B		None - Under 100K

22. Source Reference: ☒NCR (attach) ☐Action Item ☒Tech Ref. ☐GSFC ☐Other:
ECSed28075, SGI Secuirty Advispry # 20000801-02-P, Septemeber 12, 2000

23. Problem: (use additional Sheets if necessary)
SGI reported that exploitable buffer overflow has been discovered in telnetd daemon which can lead to root compromise. A local user account on the venerable systems is not required in order to exploit this telnetd daemon bug. The telnetd daemon can be exploited remotely over an un-trusted network.

Attach are the SGI Security Advisory and patch release notes

24. Proposed Solution: (use additional sheets if necessary)
SGI has released a patch for IRIX 6.2 and 6.5.X to fix this exploitable buffer overflow bug. The patches would be install like any other SGI software product via the miniroot form of the software installation tools. At the Inst> propmpt, type 'install patch SG0004050' for IRIX 6.2 systems and 'install patch SG0004060' for IRIX 6.5.x systems.

patch4060.tar = 1448936590 40960 patch4050.tar = 3292085620 1208320

25. Alternate Solution: (use additional sheets if necessary)
Turn off telnet services for all SGI platforms will prevent the exploit. This however might impact on maintenance, as it will require logging in on the system console.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)
Any SGI machine that can be access from outside ECS space can be exploited and compromise with very harmful results. One SGI machine that is root compromise would then open all the other machines to attacks. Production could be impacted severely.

27. Justification for Emergency (If Block 15 is "Emergency"):
A large number of NASA systems have already been compromised. This patch needs to be installed immediately on any ECS SGI that is connected to the DAC user LAN.

28. Site(s) Affected: ☐EDF ☒PVC ☒VATC ☒EDC ☒GSFC ☒LaRC ☒NSIDC ☒SMC ☐AK ☐JPL ☐EOC ☐IDG Test Cell ☐Other

29. Board Comments:	30. Work Assigned To:	31. CCR Closed Date:
NCR must be moved to "V" stock		

32. EDF/SCDV CCB Chair (Sign/Date):	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB
Dyan V Petes 10/4/00	
33. M&O CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
10/4/00	
34. ECS CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB

ORIGINAL

-----BEGIN PGP SIGNED MESSAGE-----

SGI Security Advisory

Title: IRIX telnetd vulnerability
Number: 20000801-02-P
Date: September 12, 2000

- --------------------
- --- Update Info ---
- --------------------

Due to a patch packaging error, patch 4044 required an unnecessary reboot after installation of the patch. Patch 4060 has been released which has the same telnetd binary fix, but the patch has been marked not to require a reboot after installation.

If you have installed patch 4044 and rebooted, there is no need to install patch 4060.

The SGI patch server sites are being updated to provide only the corrected packaged patch 4060.

The checksums below have been updated to reflect the current packaged patch 4060 values.

- ----------------------
- --- Issue Specifics ---
- ----------------------

The Last Stage of Delirium Group (http://lsd-pl.net/) has reported via BUGTRAQ that an exploitable buffer overflow has been discovered in telnetd daemon which can lead to a root compromise.

SGI has investigated the issue and recommends the following steps for neutralizing the exposure. It is HIGHLY RECOMMENDED that these measures be implemented on ALL vulnerable SGI systems. This issue will be corrected in future releases of IRIX.

- --------------
- --- Impact ---
- --------------

The telnetd daemon is installed by default on IRIX.

A local user account on the vulnerable system is not required in order to exploit telnetd daemon. The telnetd daemon can be exploited remotely

over an untrusted network.

The exploitable buffer overflow vulnerability can lead to a root compromise.

This telnetd buffer overflow vulnerability was reported by LSD on BUGTRAQ:
http://msgs.securepoint.com/cgi-bin/get/bugtraq0008/152.html
http://lsd-pl.net/files/get?IRIX/irx_telnetd

This telnetd vulnerability has been publicly discussed in Usenet newsgroups and mailing lists.

- --------------------------
- --- Temporary Solution ---
- --------------------------

Although patches are available for this issue, it is realized that there may be situations where installing the patches immediately may not be possible.

The steps below can be used to disable the telnetd daemon to prevent exploitation of this vulnerability until patches can be installed.

```
================
****  NOTE  ****
================
```

Disabling telnetd daemon will disable the telnet service.

1) Become the root user on the system.

```
% /bin/su -
Password:
#
```

2) Edit the file /etc/inetd.conf (for IRIX 5.3 and lower, edit /usr/etc/inetd.conf) with your favorite text editor. Place a "#" as the first character of the line to comment out and deactivate the telnetd daemon.

```
# vi /etc/inetd.conf
```

{Find the following line}

```
telnet stream  tcp  nowait  root  /usr/etc/telnetd  telnetd
```

{Place a "#" as the first character of the telnet line}

```
#telnet stream  tcp  nowait  root  /usr/etc/telnetd  telnetd
```

{Save the file}

3) Force inetd to re-read the configuration file.

```
# /etc/killall -HUP inetd
```

4) Kill any existing telnetd process.

```
# /etc/killall telnetd
```

5) Return to previous level.

```
# exit
%
```

- ----------------
- --- Solution ---
- ----------------

OS Version	Vulnerable?	Patch #	Other Actions
IRIX 3.x	unknown		Note 1
IRIX 4.x	unknown		Note 1
IRIX 5.0.x	unknown		Note 1
IRIX 5.1.x	unknown		Note 1
IRIX 5.2	yes	not avail	Note 1 & 3
IRIX 5.3	yes	in progress	Note 1 & 3
IRIX 6.0.x	yes	not avail	Note 1 & 3
IRIX 6.1	yes	not avail	Note 1 & 3
IRIX 6.2	yes	4050	Note 2 & 3
IRIX 6.3	yes	in progress	Note 1 & 3
IRIX 6.4	yes	in progress	Note 1 & 3
IRIX 6.5	yes	4060	Note 3 & 4
IRIX 6.5.1	yes	4060	Note 3 & 4
IRIX 6.5.2	yes	4060	Note 3 & 4
IRIX 6.5.3	yes	4060	Note 3 & 4
IRIX 6.5.4	yes	4060	Note 3 & 4
IRIX 6.5.5	yes	4060	Note 3 & 4
IRIX 6.5.6	yes	4060	Note 3 & 4
IRIX 6.5.7	yes	4060	Note 3 & 4
IRIX 6.5.8	yes	4060	Note 3 & 4
IRIX 6.5.9	yes	4060	Note 3 & 4
IRIX 6.5.10	no		Note 5

NOTES

1) This version of the IRIX operating has been retired.
   Upgrade to an actively supported IRIX operating system.
   See http://support.sgi.com/irix/news/index.html#policy
   for more information.

2) This version of the IRIX operating system is in maintenance mode.
   Upgrade to an actively supported IRIX operating system.
   See http://support.sgi.com/irix/news/index.html#policy
   for more information.

3) See "Temporary Solution" section.

4) If you have not received an IRIX 6.5.X CD for IRIX 6.5, contact your
   SGI Support Provider or download the IRIX 6.5.X Maintenance Release
   Stream from http://support.sgi.com/ or
   ftp://patches.sgi.com/support/relstream/

5) IRIX 6.5.10 is scheduled to be released in the October time-frame.

Patches are available via the web, anonymous FTP and from your SGI
service/support provider.

SGI Security Advisories can be found at:
http://www.sgi.com/support/security/ and ftp://sgigate.sgi.com/security/

SGI Security Patches can be found at:
http://www.sgi.com/support/security/ and ftp://sgigate.sgi.com/patches/

SGI patches for IRIX can be found at the following patch servers:
http://support.sgi.com/irix/ and ftp://patches.sgi.com/

SGI freeware updates for IRIX can be found at:
http://freeware.sgi.com/

SGI fixes for SGI open sourced code can be found on:
http://oss.sgi.com/projects/

SGI patches and RPMs for Linux can be found at:
http://support.sgi.com/linux/ and click on patches link or
http://oss.sgi.com/projects/sgilinux-combined/download/security-fixes/

SGI patches for Windows NT or 2000 can be found at:
http://support.sgi.com/nt/

IRIX 5.2-6.4 Recommended/Required Patch Sets can be found at:
http://support.sgi.com/irix/ and ftp://patches.sgi.com/support/patchset/

IRIX 6.5 Maintenance Release Streams can be found at:
http://support.sgi.com/irix/ and ftp://patches.sgi.com/support/relstream/

The primary SGI anonymous FTP site for security information and patches
is sgigate.sgi.com (204.94.209.1). Security information and patches can be
found in the ~ftp/security and ~ftp/patches directories, respectively.

For security and patch management reasons, ftp.sgi.com (mirror of sgigate) lags
behind and does not do a real-time update of ~ftp/security and ~ftp/patches

Patch File Checksums

The actual patch will be a tar file containing the following files:

```
Filename:                patchSG0004050
Algorithm #1 (sum -r):   29875 17 patchSG0004050
Algorithm #2 (sum):      63516 17 patchSG0004050
MD5 checksum:            C40B2DE50608C0A6C79C2167116FF76E

Filename:                patchSG0004050.eoe_man
Algorithm #1 (sum -r):   60740 74 patchSG0004050.eoe_man
Algorithm #2 (sum):      15611 74 patchSG0004050.eoe_man
MD5 checksum:            C45B59724AC5F81F5960BE78104A6B9E

Filename:                patchSG0004050.eoe_sw
Algorithm #1 (sum -r):   47453 1976 patchSG0004050.eoe_sw
Algorithm #2 (sum):      46187 1976 patchSG0004050.eoe_sw
MD5 checksum:            1D9727E9EAC3F52D56F2EC7F481D5C73

Filename:                patchSG0004050.eoe_sw64
Algorithm #1 (sum -r):   49580 104 patchSG0004050.eoe_sw64
Algorithm #2 (sum):      38983 104 patchSG0004050.eoe_sw64
MD5 checksum:            65A02D0562E0F41752363927E3CBC7F4

Filename:                patchSG0004050.idb
Algorithm #1 (sum -r):   55544 16 patchSG0004050.idb
Algorithm #2 (sum):      31605 16 patchSG0004050.idb
MD5 checksum:            143E7D4B9E38E604A4F35D504FCAFF28

Filename:                patchSG0004050.netman_data_man
Algorithm #1 (sum -r):   56900 15 patchSG0004050.netman_data_man
Algorithm #2 (sum):      58999 15 patchSG0004050.netman_data_man
MD5 checksum:            42BEB35E700813967F637E9BB0640385

Filename:                patchSG0004050.nfs_man
```

```
Algorithm #1 (sum -r):    05186 17 patchSG0004050.nfs_man
Algorithm #2 (sum):       21113 17 patchSG0004050.nfs_man
MD5 checksum:             F090E7476C01DC64F12F3A094EFAD64B

Filename:                 patchSG0004050.nfs_sw
Algorithm #1 (sum -r):    48229 83 patchSG0004050.nfs_sw
Algorithm #2 (sum):       63547 83 patchSG0004050.nfs_sw
MD5 checksum:             093B835EDC966A30980D914149BED1F0


Filename:                 README.patch.4060
Algorithm #1 (sum -r):    25834 8 README.patch.4060
Algorithm #2 (sum):       56040 8 README.patch.4060
MD5 checksum:             3933F2BD23E7938470897FB7A41A2ABA

Filename:                 patchSG0004060
Algorithm #1 (sum -r):    04186 3 patchSG0004060
Algorithm #2 (sum):       43387 3 patchSG0004060
MD5 checksum:             8C75989D7B115A2331C9BA1BC7050A6A

Filename:                 patchSG0004060.eoe_sw
Algorithm #1 (sum -r):    45231 59 patchSG0004060.eoe_sw
Algorithm #2 (sum):       33048 59 patchSG0004060.eoe_sw
MD5 checksum:             3405CD896D8988610F25B92D1B30C252

Filename:                 patchSG0004060.idb
Algorithm #1 (sum -r):    53422 1 patchSG0004060.idb
Algorithm #2 (sum):       34568 1 patchSG0004060.idb
MD5 checksum:             283FE372DC8359C7AA87EC00F9BEA48A
```

- --- Acknowledgments ----

SGI wishes to thank the users of the Internet Community at large for their assistance in this matter.

- --- SGI Security Information/Contacts ---

If there are questions about this document, email can be sent to cse-security-alert@sgi.com.

------oOo------

SGI provides security information and patches for use by the entire SGI community. This information is freely available to any person needing the information and is available via anonymous FTP and the Web.

The primary SGI anonymous FTP site for security information and patches is sgigate.sgi.com (204.94.209.1). Security information and patches are located under the directories ~ftp/security and ~ftp/patches, respectively.

The SGI Security Headquarters Web page is accessible at the URL: http://www.sgi.com/support/security/

For issues with the patches on the FTP sites, email can be sent to cse-security-alert@sgi.com.

For assistance obtaining or working with security patches, please contact your SGI support provider.

------oOo------

SGI provides a free security mailing list service called wiretap and
encourages interested parties to self-subscribe to receive (via email) all
SGI Security Advisories when they are released. Subscribing to the mailing
list can be done via the Web (http://www.sgi.com/support/security/wiretap.html)
or by sending email to SGI as outlined below.

```
% mail wiretap-request@sgi.com
subscribe wiretap <YourEmailAddress>
end
^d
```

In the example above, <YourEmailAddress> is the email address that you
wish the mailing list information sent to. The word end must be on a
separate line to indicate the end of the body of the message. The
control-d (^d) is used to indicate to the mail program that you are
finished composing the mail message.

------oOo------

SGI provides a comprehensive customer World Wide Web site. This site is
located at http://www.sgi.com/support/security/ .

------oOo------

For reporting *NEW* SGI security issues, email can be sent to
security-alert@sgi.com or contact your SGI support provider. A
support contract is not required for submitting a security report.

-----BEGIN PGP SIGNATURE-----
Version: 2.6.2

iQCVAwUBOb61p7Q4cFApAP75AQEMWgP/SMb3S601dsJ+B/M9pH7BZcS7zzYwpXvG
g/SA6CR2PD3h71wyclBPWjv89Gft5/LNvAv/1+JeXddme+9a9i9CiFDxBH1pV+5q
NyOLKq4442HEF/WucsSrparatYXcBhFs2npUp1KuZ7rvg1i03bee5eI8XgqqsPJ7
Pe+WEXaihag=
=zTLq
-----END PGP SIGNATURE-----